



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,137	07/09/2003	Boon Lum Lim	12027-0010	8102

22902 7590 08/10/2006

CLARK & BRODY
1090 VERMONT AVENUE, NW
SUITE 250
WASHINGTON, DC 20005

EXAMINER

HOMAYOUNMEHR, FARID

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/615,137

Applicant(s)

LIM, BOON LUM

Examiner

Farid Homayounmehr

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claims 1-23 have been examined.

Information Disclosure Statement PTO-1449

1. No Information Disclosure Statement was submitted by applicant.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 15 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- 3.1. Claim 15 recites the limitation "the user biometric parameter" and "the biodata". There is insufficient antecedent basis for this limitation in the claim.

- 3.2. Claim 22 is rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The claim is narrative in form and replete with indefinite and functional or operational language. The "polynomial process" is not defined in the claim or the specifications.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

5. Claims 1 to 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Willins (US Patent Application Publication No. 2002/0152391 A1), filed April 13, 2001.

5.1. As per claim 1, Willins is directed to a portable data storage device (Fig. 1 and paragraph 61) which can interface with a remote computer such as a desktop PC or a portable notebook computer (as shown in Fig.1, the mobile computer has a network module, allowing it to connect to network) and which is capable of securely storing data in digital format by reference to one or more biometric parameters (paragraphs 64 and 65 describe how the cryptographic module encrypts or decrypts data using the biometric data) and wherein such biometric parameters are encrypted by reference to a bioencryption algorithm stored within the device (paragraphs 63-65 shows how biometric parameters are encrypted) and wherein device is disposed with a biometric sensor (Fig. 1 item 11 and associated text), a biometric processing engine (Fig. 1 item 10 and associated text), a memory storage facility (Fig. 1 items 17 or 12), a micro-

Art Unit: 2132

controller (Fig. 1 item 15), a communications interface (Fig. 1 item 18), an access decision control unit (Fig. 1 item 13 and associated text), a bioparameter storage unit (Fig. 1 item 12), a combination encryption key generation means (per claim 1, the biometric key is used for encryption of data. Per claim 2 the biometric key is encrypted in the cryptographic module (see also paragraphs 64 and 65) and therefore is generated in the crypto module), a device code generation means (per paragraph 64 and claim 1, the device creates a biometric key and uses it to encrypt and decrypt user data, and therefore the device generates a code (encrypted data)), a data processing unit (Fig. 1 item 15) and a bioencryption engine (Fig. 1 item 10).

5.2. As per claims 2-9, all the elements mentioned in claim 1 are connected to one another as depicted in figure 1.

5.3. As per claims 10 and 11, the sensor receives biometric parameters from users (paragraph 59), and the sensor the sensor may be active or passive or incorporate one or more optical, capacitive, electric field, laser, infra red and or magnetic sensor and wherein the biometric sensor can scan and receive biometric parameters from users (paragraph 59).

5.4 As per claim 12, Willins is directed to a biometric processing engine as claimed in claim 1 wherein the engine comprises a processor capable of processing digital input from the sensor in accordance with predefined bioprocessing algorithms and wherein

such bioprocessed data with encryption can be stored in the memory means (Fig. 1 item 11 and item 12).

5.5 As per claim 13, Willins is directed to a memory storage means as claimed in claim 1 wherein the storage means may be volatile or non-volatile and wherein the storage means is capable of reversibly receiving and storing data for multi read/write applications (paragraph 64).

5.6 As per claim 14, Willins is directed to a bioparameters storage unit as claimed in claim 1 wherein bioparameters received from users are stored pending approval of the bioparameters prior to access to the data in the memory storage means (paragraph 63).

5.7 As per claim 15, Willins is directed to a combination encryption key generation means as claimed in claim 1 wherein the user bio-input key which is generated from the biometrics algorithm based on the user biometric parameter input and a predefined key are combined to generate a new key for encryption of the biodata (paragraph 62 describes key generation useful for encrypting the biometric data received from the user. Combining keys to generate another key is well-known in the art).

5.8 As per claim 16, Willins is directed to a device code generation means as claimed in claim 1 wherein factory preset parameters are stored (per paragraph 63, the device sends data to the network for verification and uses IPsec for secure

Art Unit: 2132

transmission. IPSec is part of the Operating System which includes factory preset data for encryption).

5.9. As per claim 17, Willins is directed to an access control decision unit as claimed in claim 1 wherein the access control decision unit evaluates biodata received by the sensor and processed by the biometric processing engine to permit or deny access to the data stored in the memory means (paragraph 63-65).

5.10. As per claim 18, Willins is directed to a bioencryption engine as claimed in claim 1 wherein bioparameters from users and factory preset parameters from the device code generator are encrypted and decrypted in accordance with predefined algorithms paragraph 65).

5.11. As per claim 19, Willins is directed to a data processing unit as claimed in claim 1 wherein data stored in the memory means is processed prior to access by a user via a communications interface (Fig. 1 item 15).

5.12. As per claim 20, Willins is directed to a micro-controller as claimed in claim 1 which comprises a processor which incorporates a communications interface whereby a user may interface the data storage device via a host computer (Fig. 1 and associated text).

5.13. As per claim 21, Willins is directed to a micro-controller as claimed in claim 20 wherein the micro-controller is disposed with a bioencryption algorithm (Fig. 10 item 10 includes an encryption algorithm).

5.14. As per claim 22, Willins is directed to a process of encryption of biometric parameters wherein biometric data from users is presented to the biometrics sensor and wherein the biometric sensor reads and transfers the biometric data to the biometric processing engine and wherein the biometric parameter is encrypted by the bioencryption engine by reference to the biometric data and a factory preset parameter in accordance with predefined algorithms in a polynomial process to produce an encryption key and wherein the encrypted biometric data is stored in the memory means (Fig. 1 item 10 and associated text. Note that generation of a key by combining other keys was well-known in the art at the time of invention).

5.15. As per claim 23, Willins is directed to a process of decryption of biometric parameters presented to the biometric sensor by a user wherein the data presented to the biometric sensor is read by the sensor and wherein the said data is then analysed by the access control decision unit in accordance with predefined parameters to ascertain whether the said biodata is in conformity with the enrolled biodata and wherein the bioencryption engine then generates a decryption key in respect of biodata verified by the access control decision unit and wherein the decryption key permits access to the data stored in the memory means (paragraph 61 to 65).

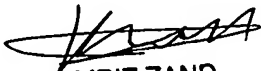
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr
Examiner


KAMBIZ ZAND
PRIMARY EXAMINER

Art Unit: 2132